REMARKS

Applicants respectfully traverse the rejection of the pending claims over Bell reference (USP 6,832,319). In that regard, consider Bell's Figure 4, which illustrates the disk manufacture process. Each disk gets a unique media ID as shown for step 40. In addition, as also explained in Col. 6, lines 50-51, all the blank disks get the same media key block (step 42 of Figure 4).

The process of forming an encrypted disk is shown in Figure 5. This process uses a disk formatted as discussed with regard to Figure 4. As seen in Figure 5 of Bell, a recorder reads the media key block from a formatted disk and determines the media key from the media key block. The recorder also reads the media ID and combines it with the media key to form a content key. The content key is then used to encrypt the data so that the resulting encrypted data may be written to the disk. The process of reading the encrypted disk is shown in Figure 6: a player reads the media key block and the media ID, determines the media key from the media key block, combines them to get the content key, and decrypts the encrypted data using the content key.

But note the flaw in the Bell system: anyone with access to a disk reader may obtain the media key block and the media ID. Having read the media key, a hacker may then freely experiment using various hacking algorithms to get the media key. The hacker may then proceed to combine the hacked media key with the media ID to get the content key.

In sharp contrast, claim 1 recites the acts of "generating a pseudo-random number within the data storage engine" and "generating an internal key within the data storage engine using the pseudo-random number generator." (no new matter is added, claim 1 being amended to recite the internal pseudo-random number generation recited, for example, in claim 20). Thus, the generation of the internal key has nothing to do with reading data from the disk. A hacker may read the disk's contents exhaustively but never will have access to the

-7-   Appl. No.: 09/583,452

internal key generation. As set forth on page 10, lines 1 through 12, even if a hacker reverse engineers the ASIC that performs the pseudo-random number generation, the seed to the number generator may be stored externally to the ASIC, thereby defeating even this advanced hacking act. In this fashion, the digital rights management is "storage-engine-based" as compared to the host-based scheme in the Bell reference in which a manufacturer (rather than the storage engine) provides the media key block. Accordingly, claim 1 is patentable over the Bell reference.
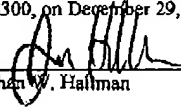
The Silverbrook reference (USP 6,334,190) does nothing to cure the deficiencies of the Bell reference. Thus, because claims 2 and 6 – 13 depend either directly or indirectly upon claim 1, these claims are patentable over the cited prior art for at least the same reasons.

Claim 14 and its dependent claims 15 – 19 are patentable over the cited prior art analogously as discussed with regard to claim 1. For example, claim 14 recites the act of "generating a plurality of internal keys using the pseudo-random number generator." For analogous reasons, claim 20 and its dependent claim 21 are patentable over the cited prior art.

-8-   **Appl. No.: 09/583,452**

CONCLUSION

For the above reasons, pending Claims 1 – 2, and 6 – 21 are in condition for allowance and allowance of the application is hereby solicited. If the Examiner has any questions or concerns, a telephone call to the undersigned at (949) 752-7040 is welcomed and encouraged.

I hereby certify that this correspondence is facsimile transmitted to the Commissioner for Patents, Washington, D.C. 20231, at 571-273-8300, on December 29, 2005.

_____   December 29, 2005
Jonathan W. Hallman   Date of Signature

Respectfully submitted,

Jonathan W. Hallman
Attorney for Applicant(s)
Reg. No. 42,622

-9-   **Appl. No.: 09/583,452**